Product Service Laboratory

Automotive Cybersecurity
Connected Vehicles and the IOT

Intertek
Valued Quality. Delivered.

Identifying Future Problems Today

According to a McAfee white paper*, "when an object as complex as a car is connected to the internet assessing the scope of threats is a massive job potentially leaving countless security vulnerabilities exposed to attackers." Most modern vehicles have "100 or more ECUs (Electronic Control Unit) that interface with most if not all in-vehicle systems and (are) often exposed to multiple types of external networks like cellular (GSM, CDMA, LTE etc), Wifi (802.11), car maintenance employees using hand held service devices, toll road smart devices, and more."

Specific Capabilities/Equipment

- Perform an architectural review of the OEM or Tier supplier platform and identify areas needed to be "hardened"
- Use automated tools for penetration testing trying to overwhelm the system and highlight issues
- Reverse engineering of existing vehicle parameters on vehicle communication systems
- 25+ years of device testing - device to vehicle interoperability, app interoperability, app and device security, device to network interoperability, global field trials
- Access to 3400+ devices (mobile & connected things) for access pairing, connectivity and interoperability
- Global capabilities with facilities located in Pennsylvania, California, Michigan (USA), Milton Keynes (UK), Kaufbeuren (Germany), Hong Kong (China) and Tokyo (Japan)

Areas of Significant Cybersecurity Risk

McAfee* highlights the 15 "most hackable and exposed surfaces" on a modern car: Remote Link Type App, Airbag ECU, OBD II, USB, Bluetooth, DSRC-Based Receiver, Passive Keyless Entry, Remote Key Entry, TPMS, ADAS System ECU, Lighting System ECU, Engine and Transmission ECU, Steering and Breaking ECU, Vehicle Access System ECU, User's Smartphone

A high level look at areas of significant risk for cybersecurity breach include:

- Secure Boot - Works with the hardware to ensure that the loaded software components are valid to provide a root of trust for the rest of the system.
- Hardware Security - Secure boot and software attestation functions: Detects tampering with boot loaders and critical operating system files by checking their digital signatures and product keys.
- Network Security - Message authentication: Verifies that communications are coming from the approved source and defenses to protect authentications from being spoofed or recorded and replayed.
- Cloud Security - Secure authenticated channel to the cloud: Leverages hardware-assisted cryptography for remote monitoring, software updates, and other communications.

McAfee "Automotive Security Best Practices" White Paper

For more information, please contact:

icenter@intertek.com
1-800-WORLDLAB (967-5352)
intertek.com/automotive